



FortiSwitch Release Notes

Version 3.6.9

FORTINET DOCUMENT LIBRARY

<http://docs.fortinet.com>

FORTINET VIDEO GUIDE

<http://video.fortinet.com>

FORTINET BLOG

<https://blog.fortinet.com>

CUSTOMER SERVICE & SUPPORT

<https://support.fortinet.com>

FORTIGATE COOKBOOK

<http://cookbook.fortinet.com>

FORTINET TRAINING SERVICES

<http://www.fortinet.com/training>

FORTIGUARD CENTER

<http://www.fortiguard.com>

END USER LICENSE AGREEMENT

<http://www.fortinet.com/doc/legal/EULA.pdf>

FEEDBACK

Email: techdocs@fortinet.com



November 8, 2019

FortiSwitch 3.6.9 Release Notes

11-369-519789-20191108

TABLE OF CONTENTS

- Change log** 4
- Introduction** 5
 - Supported models 5
 - What’s new in 3.6.9 5
- Special notices** 6
 - Supported features for FortiSwitchOS 3.6 6
 - Connecting multiple FSW-R-112D-POE switches11
- Upgrade information**12
 - Cooperative Security Fabric upgrade 12
- Product integration and support** 13
 - FortiSwitch 3.6.9 support 13
- Resolved issues**14
 - Common vulnerabilities and exposures 14
- Known issues**15

Change log

Date	Change Description
November 20, 2018	Initial document release for FortiSwitchOS 3.6.9
December 6, 2018	Updated the “Supported models” section.
February 5, 2019	Added bug 535736 to the “Known Issues” section.
November 8, 2019	Added bug 593993 to the “Known Issues” section.

Introduction

This document provides the following information for FortiSwitch 3.6.9 build: 0426.

- [Supported models on page 5](#)
- [Special notices on page 6](#)
- [Upgrade information on page 12](#)
- [Product integration and support on page 13](#)
- [Resolved issues on page 14](#)
- [Known issues on page 15](#)

See the [Fortinet Document Library](#) for FortiSwitch documentation.

Supported models

FortiSwitch 3.6.9 supports the following models:

FortiSwitch	FSW-108D-POE, FSW-108E, FSW-108E-POE, FSW-108E-FPOE, FSW-124D, FSW-124D-POE, FSW-124E, FSW-124E-POE, FSW-124E-FPOE, FSW-224D-FPOE, FSW-224D-POE, FSW-224E, FSW-224E-POE, FSW-248D-FPOE, FSW-248D-POE, FSW-248D, FSW-248E-POE, FSW-248E-FPOE, FSW-424D, FSW-424D-FPOE, FSW-424D-POE, FSW-448D, FSW-448D-FPOE, FSW-448D-POE, FSW-524D-FPOE, FSW-524D, FSW-548D, FSW-548D-FPOE, FSW-1024D, FSW-1048D, FSW-1048E, FSW-3032D
FortiSwitch Rugged	FSR-112D-POE, FSR-124D

What's new in 3.6.9

FortiSwitch 3.6.9 is a patch release only. No new features or enhancements have been implemented in this release.

Special notices

Supported features for FortiSwitchOS 3.6

The following table lists the FortiSwitch features in Release 3.6 that are supported on each series of FortiSwitch models. All features are available in Release 3.6.0, unless otherwise stated.

Feature	GUI supported	108D-POE 112D-POE 224D-POE	1xxE	124D 124D-POE 200 Series 400 Series	500 Series	1024D 1048D 1048E	3032D
Link aggregation group size (maximum number of ports) (See Note 2.)	✓	8	8	8	24/48	24/48	24 (3.5.0) 64 (3.5.1)
Auto module max speed detection and notification	✓	—	—	—	✓	✓	—
IP conflict detection and notification	—	✓	✓	✓	✓	✓	✓
IP-MAC binding	✓	—	—	—	✓	✓	✓
Static BFD	—	—	—	—	—	✓	✓
Hardware-based ECMP	—	—	—	—	✓	✓	✓
Private VLANs	✓	—	—	✓	✓	✓	✓
LLDP transmit	—	✓	—	✓	✓	✓	✓
Loop guard	✓	✓	✓	✓	✓	✓	✓
LAG min-max-bundle	—	✓	✓	✓	✓	✓	✓
sFlow	✓	✓	—	✓	✓	✓	✓
Storm control	✓	✓	✓	✓	✓	✓	✓
ACL	—	—	—	✓	✓	✓	✓
Static L3/hardware-based routing	✓	—	—	✓	✓	✓	✓

Feature	GUI supported	108D-POE 112D-POE 224D-POE	1xxE	124D 124D-POE 200 Series 400 Series	500 Series	1024D 1048D 1048E	3032D
Software routing only	✓	✓	✓	—	—	—	—
CPLD software upgrade support for OS	—	—	—	—	—	1024D 1048D	—
PoE-pre-standard detection (See Note 1.)	✓	✓	FS-1xxE POE	✓	✓	—	—
VLAN tag by ACL	—	—	—	✓	✓	✓	✓
ACL redirect to mirror destination as trunk/LAG	—	—	—	✓	✓	✓	✓
MAC/IP/protocol-based VLAN assignment	✓	✓	—	✓	✓	✓	✓
802.1x port mode	✓	✓	✓	✓	✓	✓	✓
802.1x MAC-based security mode	✓	✓	✓	✓	✓	✓	✓
User-based (802.1x) VLAN assignment	✓	✓	—	✓	✓	✓	✓
Virtual wire	✓	—	—	✓	✓	✓	✓
HTTP REST APIs for configuration and monitoring	—	✓	✓	✓	✓	✓	✓
Split port	—	—	—	—	✓	—	✓
IGMP snooping	—	—	—	✓	✓	✓	✓
Per-port max for learned MACs	—	—	✓	✓	✓	—	—
802.1p support, including priority queuing trunk and WRED (release 3.5.1)	—	—	—	✓	✓	✓	✓
DHCP snooping	—	—	—	✓	✓	✓	✓
LLDP-MED	—	✓	✓	✓	✓	✓	✓
DHCP relay feature	—	—	✓	✓	✓	✓	✓

Feature	GUI supported	108D-POE 112D-POE 224D-POE	1xxE	124D 124D-POE 200 Series 400 Series	500 Series	1024D 1048D 1048E	3032D
Support for switch SNMP OID	—	✓	✓	✓	✓	✓	✓
Access VLANs (See Note 5.)	—	—	—	✓	✓	✓	✓
802.1x enhancements, including MAB (release 3.5.1)	✓	✓	✓	✓	✓	✓	✓
Multi-stage load balancing (release 3.5.1)	—	—	—	—	—	✓	✓
MCLAG (multichassis link aggregation)(release 3.6.0)	—	—	—	✓ (not on 124D/124D-POE)	✓	✓	✓
Dynamic layer-3 protocols (OSPF, RIP, and VRRP) (release 3.6.0) (See Note 3.)	✓	—	—	✓ (not on 124D/124D-POE)	✓	✓	✓
Dynamic ARP inspection (release 3.6.0)	—	—	—	✓	✓	✓	✓
Firmware image rotation (dual-firmware image support) (release 3.6.0)	—	✓ (not on 108D-POE)	—	✓	✓	✓	✓
TDR (time-domain reflectometer)/cable diagnostics support (release 3.6.0)	✓	—	—	✓	✓	✓	✓
MAC learning limit (release 3.6.0) (See Note 4.)	—	—	✓	✓	✓	—	—
Sticky MAC on switch interfaces (release 3.6.0)	—	—	—	✓	✓	✓	✓

Feature	GUI supported	108D-POE 112D-POE 224D-POE	1xxE	124D 124D-POE 200 Series 400 Series	500 Series	1024D 1048D 1048E	3032D
PoE modes support: first come, first served or priority based (PoE models) (release 3.6.0)	—	✓	FS-1xxE POE	✓	✓	—	—
ACL: egress mask action support (release 3.6.0)	—	—	—	✓	✓	✓	✓
Monitor system temperature (threshold configuration and SNMP trap support) (release 3.6.0)	—	✓	—	✓	✓	✓	✓
'forced-untagged' or 'force-tagged' setting on switch interfaces (release 3.6.0)	—	✓	—	✓	✓	✓	✓
Selective packet sampling to CPU (useful diagnostic tool) (release 3.6.0)	—	—	—	✓	✓	✓	3.6.1
Add CLI to show the details of port statistics (release 3.6.0)	—	✓	✓	✓	✓	✓	✓
Display progress (%) during firmware upgrade (release 3.6.0)	✓	✓	✓	✓	✓	✓	✓
STP root guard (release 3.6.2)	—	✓	✓	✓	✓	✓	✓
STP BPDU guard (release 3.6.2)	—	✓	✓	✓	✓	✓	✓
IGMP snooping: static multicast groups (release 3.6.2)	—	—	—	✓	✓	✓	✓
DHCP snooping: entry limit per port (release 3.6.2)	—	—	—	✓	✓	✓	✓

Feature	GUI supported	108D-POE 112D-POE 224D-POE	1xxE	124D 124D-POE 200 Series 400 Series	500 Series	1024D 1048D 1048E	3032D
Network device detection (release 3.6.2)	—	—	—	✓	✓	✓	✓
QoS queue counters (releases 3.6.2 and 3.6.3)	—	—	—	✓	✓	✓	✓
Support of the RADIUS accounting server (release 3.6.3)	—	✓	—	✓	✓	✓	✓
Support of RADIUS CoA and disconnect messages (release 3.6.3)	—	✓	—	✓	✓	✓	✓
802.1x authentication: EAP-TLS support (release 3.6.3)	—	✓	—	✓	✓	✓	✓
DHCP snooping: CLI for DHCP-snooping server database (release 3.6.3)	—	—	—	✓	✓	✓	✓
Unicast hashing (release 3.6.4)	—	—	—	✓	✓	✓	✓
STP supported in MCLAGs (release 3.6.4)	—	—	—	✓ (not on 124D/124D-POE)	✓	✓	✓
QoS marking (release 3.6.4)	—	—	—	✓	✓	✓	✓
MAB reauthentication disabled (release 3.6.4)	—	✓	—	✓	✓	✓	✓
Cut-through switching (release 3.6.4)	—	—	—	—	—	✓	✓
Control of temperature and PoE alerts (release 3.6.4)	—	✓	—	✓	✓	✓	✓
IGMP querier (release 3.6.4)	—	—	—	✓	✓	✓	✓

Feature	GUI supported	108D-POE 112D-POE 224D-POE	1xxE	124D 124D-POE 200 Series 400 Series	500 Series	1024D 1048D 1048E	3032D
Configuration of the QSFP low-power mode (release 3.6.4)	—	—	—	—	✓	1048D	✓
Learning limit violation log (release 3.6.4) (See Note 4.)	—	—	—	✓	✓	—	—
Sticky MAC addresses saved to static MAC table (release 3.6.4)	—	—	—	✓	✓	✓	✓
Enabling packet forwarding to CPU (release 3.6.4)	—	—	—	✓	—	—	—

Notes

1. PoE features are applicable only to the model numbers with a POE or FPOE suffix.
2. 24-port LAG is applicable to 524D, 524_FPOE, 1024D, and 3032D models. 48-port LAG is applicable to 548D, 548-FPOE, and 1048D models.
3. To use the dynamic layer-3 protocols, you must have an advanced features license.
4. The per-VLAN learning limit and per-trunk learning limit are not supported on dual-chip platforms (248 and 448 series).
5. Access VLANs are not supported on 108D-POE, 224D-POE, or 112D-POE.

Connecting multiple FSW-R-112D-POE switches

The FSW-R-112D-POE switch does not support interconnectivity to other FSW-R-112D-POE switches using the PoE ports. Fortinet recommends using the SFP ports to interconnect switches.

Upgrade information

FortiSwitch 3.6.9 supports upgrading from FortiSwitch 3.5.0 and later.

Cooperative Security Fabric upgrade

FortiOS 5.4.1 greatly increases the interoperability between other Fortinet products. This includes:

- FortiClient 5.4.1
- FortiClient EMS 1.0.1
- FortiAP 5.4.1
- FortiSwitch 3.4.2

The upgrade of the firmware for each product must be completed in a precise order so the network connectivity is maintained without the need of manual steps. Customers must read the following two documents prior to upgrading any product in their network:

- *Cooperative Security Framework - Upgrade Guide*
- *FortiOS 5.4.0 to 5.4.1 Upgrade Guide for Managed FortiSwitch Devices*

This document is available in the Customer Support Firmware Images download directory for FortiSwitch 3.4.2.

Product integration and support

FortiSwitch 3.6.9 support

The following table lists 3.6.9 product integration and support information.

Web browser	<ul style="list-style-type: none">• Microsoft Internet Explorer version 11• Mozilla Firefox version 52• Google Chrome version 56 <p>Other web browsers may function correctly, but are not supported by Fortinet.</p>
FortiOS (FortiLink Support)	FortiLink is supported on all FortiSwitch models when running FortiOS 5.4.0 and later and FortiSwitchOS 3.2.1 and later.

Resolved issues

The following issues have been fixed in 3.6.9. For inquiries about a particular bug, please contact [Customer Service & Support](#).

Bug ID	Description
464703, 508490	The PoE_Max LED does not light up when the PoE exceeds its alarm threshold.
497248	After enabling mclag-stp-aware, there are “STP state DISCARDING” errors, and some switches go down.
505451	LACP trunks are periodically reset on the FortiSwitch unit.
506762	The FortiSwitch unit cannot be accessed through the GUI or SSH after an IP camera is connected to it.
507257, 511286, 514884, 515100, 515388, 518410	Managed switches randomly go down until the switch-controller CAPWAP control daemon is restarted on the switch.
510229	A user cannot ping between D-series switches and E-series switches when they have different native VLAN configurations on the internal interface and uplink interface.
517534	When VRRP is running on a FortiSwitch unit, an IP conflict is incorrectly reported.
520300	When you add a new mirror or edit an existing mirror, port1 cannot be added.

Common vulnerabilities and exposures

FortiSwitchOS 3.6.9 is no longer vulnerable to the following CVEs:

- CVE-2018-15473
- CVE-2015-9251
- CVE-2012-6708

Visit <https://fortiguard.com/psirt> for more information.

Known issues

The following known issues have been identified with 3.6.9. For inquiries about a particular bug or to report a bug, please contact [Fortinet Customer Service & Support](#).

Bug ID	Description
380239	IGMP-snooped multicast groups are not immediately flushed out of the snooping table when the querier port is shut down.
391607	Switch does not send gratuitous ARP for IP conflict when the system boots up and adds a new switch virtual interface (SVI).
414972	IGMP snooping might not work correctly when used with the 802.1x dynamic VLAN functionality in the 802.1x MAC-based authentication.
416655	When using DHCP, the IPv6 address cannot be configured. Also, the automatic configuration of the global address does not work.
424432	When MCLAG is enabled In FortiLink mode, IGMP reports are not synchronized if the <code>igmps-report-flood</code> and <code>igmps-traffic-flood</code> options are disabled the the FortiLink/ISL/MCLAG trunks.
438441	DHCP snooping and dynamic ARP inspection (DAI) do not work with private VLANs (PVLANS).
509787	FortiSwitch Cloud is disabled when upgrading FortiSwitch firmware.
510943	When using the cable diagnostics feature on a port (with the <code>diagnose switch physical-ports cable-diag <physical port name></code> CLI command), ensure that the physical link on its neighbor port is down. You can disable the neighbor ports or physically remove the cables.

Bug ID	Description
535736	<p>If a FortiSwitch firmware image is an even multiple of 1024 bytes, it will not upgrade properly using the default FortiLink upgrade mechanism. The following builds are known to be affected:</p> <p>version 3.x build 0415/FSW_124D_POE</p> <p>version 6.x build 0039/FSW_1048E build 0043/FSW_124E build 0141/FSW_224D_FPOE build 0052/FSW_548D_FPOE</p> <p>Workaround: Change to HTTPS mode using the following commands:</p> <pre>config switch-controller global set https-image-push enable end</pre>
593993	<p>When the switch-controller.global.https-image-upgrade is enabled, the FS-108D-POE/FS-224D-POE might fail to upgrade.</p> <p>Workaround: Disable https-image-upgrade.</p>



Copyright© 2019 Fortinet, Inc. All rights reserved. Fortinet®, FortiGate®, FortiCare® and FortiGuard®, and certain other marks are registered trademarks of Fortinet, Inc., in the U.S. and other jurisdictions, and other Fortinet names herein may also be registered and/or common law trademarks of Fortinet. All other product or company names may be trademarks of their respective owners. Performance and other metrics contained herein were attained in internal lab tests under ideal conditions, and actual performance and other results may vary. Network variables, different network environments and other conditions may affect performance results. Nothing herein represents any binding commitment by Fortinet, and Fortinet disclaims all warranties, whether express or implied, except to the extent Fortinet enters a binding written contract, signed by Fortinet's General Counsel, with a purchaser that expressly warrants that the identified product will perform according to certain expressly-identified performance metrics and, in such event, only the specific performance metrics expressly identified in such binding written contract shall be binding on Fortinet. For absolute clarity, any such warranty will be limited to performance in the same ideal conditions as in Fortinet's internal lab tests. In no event does Fortinet make any commitment related to future deliverables, features or development, and circumstances may change such that any forward-looking statements herein are not accurate. Fortinet disclaims in full any covenants, representations, and guarantees pursuant hereto, whether express or implied. Fortinet reserves the right to change, modify, transfer, or otherwise revise this publication without notice, and the most current version of the publication shall be applicable.